Notice of Allowability	Application No.	Applicant(s)	
	09/849,403	JIANG, SAM SHIAW-SHIANG	
	Examiner	Art Unit	
	Ronald Baum	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *7/23/04*.

2. ☒ The allowed claim(s) is/are *1-3,5,7-14,16-19 and 25-31*.

3. ☐ The drawings filed on _____ are accepted by the Examiner.

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

6. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *11022004* .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Winston Hsu, Reg. No. 41,526 on 10/13/2004.

1. Replace claims 1,5,11,12,14 with:

1. A method for synchronizing a ciphering key change in a wireless communications system, the wireless communications system comprising:

a first station capable of receiving a security mode command to effect a ciphering change, and capable of receiving encrypted layer 2 protocol data units (PDUs), each received PDU being sequentially identified by an n-bit frame number (FN), the first station comprising:

a decryption unit capable of decrypting received PDUs according to at least a first ciphering key, a first m-bit hyper frame number (HFN) which is a function of the FN for each received PDU, and the FN of each received PDU; and

a second station capable of transmitting the security mode command, capable of assigning each transmitted PDU with an n-bit FN and capable of transmitting encrypted PDUs, the second station comprising:

an encryption unit capable of encrypting transmitted PDUs according to at least the first ciphering key, a second m-bit HFN which is a function of the FN for each transmitted PDU and is synchronized with the first m-bit HFN, and the FN associated with each transmitted PDU;

the method comprising:

the second station determining an activation time at which a ciphering key change is to occur, the activation time corresponding to a second HFN/FN sequence pair for a crossover PDU, the crossover PDU being the sequentially earliest PDU encrypted using a second ciphering key;

the second station composing the security mode command, the security mode command comprising a switching FN corresponding to the activation time, and x least-significant bits (LSBs) from the second HFN corresponding to the crossover PDU;

the second station transmitting the security mode command;

the first station receiving the security mode command;

the first station utilizing the switching FN and the x LSBs from the second HFN contained in the security mode command to obtain an application time; and

the first station using the first ciphering key to decrypt PDUs with FNs sequentially prior to the application time, and using the second ciphering key to decrypt PDUs with FNs sequentially on or after the application time, wherein the second ciphering key is different from the first ciphering key.

5. The method of claim 1 wherein the application time corresponds to a synchronized first HFN/FN sequence pair for a corresponding received PDU.

11. A wireless communications system comprising:

a first station capable of receiving encrypted layer 2 protocol data units (PDUs), and capable of receiving a security mode command, the first station comprising:

a receiving buffer for storing received PDUs;

a means for associating a sequentially ordered n-bit frame number (FN) with each received PDU by the first station;

a means for maintaining an m-bit hyper frame number (HFN) as a function of the associated FN for each received PDU by the first station;

an extraction unit for obtaining an application time from a switching FN and x least significant bits (LSBs) of a second HFN, the switching FN being the FN of a crossover PDU and the second HFN being the HFN of the crossover PDU, the switching FN and the x LSBs of the second HFN being contained in the security mode command;

a means for storing a first ciphering key;

a means for storing a second ciphering key, the second ciphering key being different from the first ciphering key;

a second station capable of transmitting encrypted layer 2 PDUs, and capable of transmitting a security mode command, the second station comprising:

an encryption unit capable of generating an activation time, the activation time corresponding to an HFN/FN sequence pair for the crossover PDU, the crossover PDU being the sequentially earliest PDU encrypted by the encryption unit using the second ciphering key; and

a decryption unit for decrypting the received PDUs, the decryption unit using the first ciphering key to decrypt any received PDU with an HFN/FN pair that is sequentially before the application time, and using the second ciphering key to decrypt any received PDU with an HFN/FN pair that is sequentially on or after the application time.

12. The system of claim 11 wherein PDUs that are sequentially before the application time are encrypted using the first ciphering key, and PDUs sequentially on or after the application time are encrypted using the second ciphering key.

14. The system of claim 11 wherein the application time corresponds to a synchronized HFN/FN sequence pair for a corresponding PDU received by the first station.

2. Cancel claims 4,6,15.

Examiner's Statement of Reasons for Allowance

3. Claims 1-3,5,7-14,16-19 and 25-31 are allowed over prior art.

4. This action is in reply to applicant's correspondence of 23 July 2004.

5. The following is an examiner's statement of reasons for the indication of allowable claimed subject matter.

6. As per claims 1,11,25, prior art of record, Finkelstein et al, U.S. Patent 5,319,712 fails to teach, alone, or in combination, of;

(claim 1) "A *method for synchronizing a ciphering key change in a wireless communications system*, the wireless communications system comprising:

a first station capable of receiving a security mode command to effect a ciphering change, and capable of receiving encrypted layer 2 protocol data units (PDUs), each received PDU being sequentially identified by an n-bit frame number (FN), the first station comprising:

a decryption unit capable of decrypting received PDUs according to at least a first ciphering key, a first m-bit hyper frame number (HFN) which is a function of the FN for each received PDU, and the FN of each received PDU; and

a second station capable of transmitting the security mode command, capable of assigning each transmitted PDU with an n-bit FN and capable of transmitting encrypted PDUs, the second station comprising:

an encryption unit capable of encrypting transmitted PDUs according to at least the first ciphering key, *a second m-bit HFN which is a function of the FN for*

each transmitted PDU and is synchronized with the first m-bit HFN, and the FN associated with each transmitted PDU;

the method comprising:

the second station *determining an activation time at which a ciphering key change is to occur, the activation time corresponding to a second HFN/FN sequence pair for a crossover PDU, the crossover PDU being the sequentially earliest PDU encrypted using a second ciphering key*;

the second station composing the security mode command, the security mode command comprising a *switching FN corresponding to the activation time, and x least-significant bits (LSBs) from the second HFN corresponding to the crossover PDU*;

the second station transmitting the security mode command;

the first station receiving the security mode command;

the *first station utilizing the switching FN and the x LSBs from the second HFN contained in the security mode command to obtain an application time*; and

the first station using the *first ciphering key to decrypt PDUs with FNs sequentially prior to the application time, and using the second ciphering key to decrypt PDUs with FNs sequentially on or after the application time, wherein the second ciphering key is different from the first ciphering key.*"

(claim 11) "A wireless communications system comprising:

a first station capable of receiving encrypted layer 2 protocol data units (PDUs), and capable of receiving a security mode command, the first station comprising:

a receiving buffer for storing received PDUs;

a means for associating a sequentially ordered n-bit frame number (FN) with each received PDU by the first station;

a means for maintaining an m-bit hyper frame number (HFN) as a function of the associated FN for each received PDU by the first station;

an extraction unit for obtaining an application time from a switching FN and x least significant bits (LSBs) of a second HFN, the switching FN being the FN of a crossover PDU and the second HFN being the HFN of the crossover PDU, the switching FN and the x LSBs of the second HFN being contained in the security mode command;

a means for storing a first ciphering key;

a means for storing a second ciphering key, the second ciphering key being different from the first ciphering key;

a second station capable of transmitting encrypted layer 2 PDUs, and capable of transmitting a security mode command, the second station comprising:

an encryption unit capable of generating an activation time, the activation time corresponding to an HFN/FN sequence pair for the crossover PDU, the crossover PDU being the sequentially earliest PDU encrypted by the encryption unit using the second ciphering key; and

a decryption unit for decrypting the received PDUs, the decryption unit using the first ciphering key to decrypt any received PDU with an HFN/FN pair that is sequentially before the application time, and using the second ciphering key to decrypt any received PDU with an HFN/FN pair that is sequentially on or after the application time."

(claim 25) "A method for *removing cyclical ambiguity of an n-bit identifying frame number (FN) transmitted in a signaling message* from a first station to a second station in a wireless communications system, the method comprising:

the first station placing an identifying FN for identifying a layer 2 protocol data unit (PDU) in a stream of transmitted PDUs, into a first field of a message;

the first station placing *x least significant bits (LSBs) from a first m-bit hyper frame number (HFN) value associated with the identifying FN in a second field of the message, the first HFN being incremented by a first value upon detection of roll-over of an FN in the stream of transmitted PDUs*; and

the first station transmitting the message to the second station;

the second station receiving the message and *using the x LSBs of the second field to determine a cyclical position of the identifying FN of the first field;*

wherein x<m."

The italicized above claim elements dealing with (for example; claim 1) " ... *A method for synchronizing a ciphering key change in a wireless communications system, ... a first m-bit*

hyper frame number (HFN) which is a function of the FN for each received PDU, and the FN of each received PDU; ... a second m-bit HFN which is a function of the FN for each transmitted PDU and is synchronized with the first m-bit HFN, and the FN associated with each transmitted PDU; ... determining an activation time at which a ciphering key change is to occur, the activation time corresponding to a second HFN/FN sequence pair for a crossover PDU, the crossover PDU being the sequentially earliest PDU encrypted using a second ciphering key; ... switching FN corresponding to the activation time, and x least-significant bits (LSBs) from the second HFN corresponding to the crossover PDU; ... first station utilizing the switching FN and the x LSBs from the second HFN contained in the security mode command to obtain an application time; ... first ciphering key to decrypt PDUs with FNs sequentially prior to the application time, and using the second ciphering key to decrypt PDUs with FNs sequentially on or after the application time, wherein the second ciphering key is different from the first ciphering key. ..." serving to patently distinguish the invention from prior art. Specifically, the use of synchronizing a ciphering key change in a wireless communications system using encrypted layer 2 protocol data units (PDUs) with associated frame numbers (FN) / hyper frame numbers (HFN) synchronization is taught in the prior art. However, as per the applicants arguments in the previous remarks in the Amendment (July 23, 2004), the examiner finds the applicant's arguments to be persuasive in that a method / system for cipher key changing many times within one connection session, and further that the first/second FN specifically synchronized at the crossover PDU at key activation time, with the "x LSBs are extracted from the second HFN corresponding to the crossover PDU", patently distinguishing the invention from prior art. Claim 11 deals with system for the method of claim 1, and claim 25 deals with the

specific problem solution for using the method of the application of "removing cyclical ambiguity" involved in the keying in a synchronized crossover of PDUs at key activation time, given, "using the x LSBs of the second field to determine a cyclical position of the identifying FN of the first field; wherein x<m.".

Dependent claims 7-10,18-20, 28-29 are allowable by virtue of their dependencies.

Conclusion

7. Any inquiry concerning this communication or earlier communications from examiner should be directed to Ronald Baum, whose telephone number is (703) 305-4276. The examiner can normally be reached Monday through Friday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh, can be reached at (703) 305-9648. The Fax number for the organization where this application is assigned is 703-872-9306.

Ronald Baum

Patent Examiner

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100